

(19) RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
PARIS

(11) N° de publication : 2 793 904  
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : 99 06499

(51) Int Cl<sup>7</sup> : G 06 F 12/14, G 11 C 7/24, 7/10

(12)

## DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 21.05.99.

(30) Priorité :

(71) Demandeur(s) : STMICROELECTRONICS SA  
Société anonyme — FR.

(72) Inventeur(s) : WUIDART SYLVIE.

(43) Date de mise à la disposition du public de la demande : 24.11.00 Bulletin 00/47.

(56) Liste des documents cités dans le rapport de recherche préliminaire : Se reporter à la fin du présent fascicule

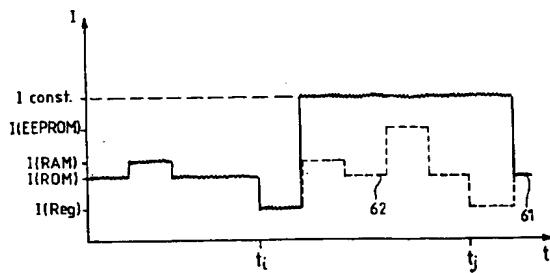
(60) Références à d'autres documents nationaux apparentés :

(73) Titulaire(s) :

(74) Mandataire(s) : CABINET BALLOT SCHMIT.

### (54) PROCEDE ET DISPOSITIF DE GESTION D'UN CIRCUIT ELECTRONIQUE.

(57) L'invention propose un procédé de gestion d'un circuit électronique du type comprenant une mémoire (EEPROM) pour le stockage d'informations confidentielles, procédé comprenant le masquage des variations du courant électrique ( $I$ ) consommé par le circuit électronique, pendant une fraction du temps seulement ( $t_i - t_j$ ), et en tout état de cause pendant la ou les portions du temps pendant lesquelles est exécutée, entre autres, une instruction portant sur des données confidentielles, notamment une instruction de lecture dans la mémoire (EEPROM).



FR 2 793 904 - A1



**PROCEDE ET DISPOSITIF DE GESTION D'UN CIRCUIT ELECTRONIQUE**

La présente invention concerne un procédé et un dispositif de gestion d'un circuit électronique, notamment un microcontrôleur, du type comprenant une mémoire pour le stockage permanent d'informations confidentielles.

5 A la figure 1 on a représenté le schéma de l'architecture interne d'un tel circuit électronique. Une unité centrale de traitement CPU ("Central Processing Unit", en anglais) échange des informations avec des organes périphériques internes par l'intermédiaire d'un bus de données DB. Ces organes  
10 périphériques comprennent une première mémoire non volatile ROM pour le stockage permanent d'un programme de gestion, qui est une mémoire à lecture seule ("Read-Only-Memory", en anglais). Ils comprennent également une seconde mémoire non volatile EEPROM pour le stockage permanent d'informations  
15 confidentielles, qui est une mémoire électriquement programmable et effaçable à lecture seule ("Electricaly Erasable and Programmable Read-Only-Memory", en anglais). Ils comprennent en outre une mémoire volatile RAM pour le stockage temporaire d'informations liées au fonctionnement du circuit,  
20 qui est une mémoire à accès aléatoire ("Random Access Memory", en anglais). En général, ils comprennent encore au moins un registre Reg pour le stockage d'une information binaire.

L'invention s'applique notamment à un microcontrôleur de carte à puce. Les informations confidentielles stockées dans  
25 la mémoire EEPROM sont par exemple un code personnel connu de l'utilisateur seulement. Ce code personnel doit être fourni par l'utilisateur pour utiliser un appareil tel qu'un distributeur de billets, un décodeur pour télévision à péage, un téléphone portatif de type GSM, etc..., en combinaison avec  
30 la carte à puce.

La carte à puce est classiquement insérée dans un lecteur de carte à puce de l'appareil. La carte à puce comporte des pastilles de contact coopérant avec des bornes correspondantes du lecteur pour l'échange d'informations entre la carte et le  
35 lecteur, et pour l'alimentation électrique de la carte à puce à l'aide d'une source d'alimentation électrique du lecteur.

L'appareil comporte un clavier ou dispositif analogue sur lequel l'utilisateur saisit son code personnel. Le code personnel saisi par l'utilisateur est transmis au microcontrôleur de la carte à puce qui comporte des moyens pour le comparer au code personnel stocké dans la mémoire EEPROM. En cas d'égalité, l'accès au service délivré par l'appareil est permis à l'utilisateur.

Une tentative de fraude classique consiste à utiliser une carte à puce volée dans un lecteur de carte à puce pirate, comprenant des moyens pour observer les données placées sur le bus de données DB. Il est alors théoriquement possible de relever sur le bus de données DB les données confidentielles correspondant au code personnel de l'utilisateur lorsque ces données sont lues dans la mémoire EEPROM et sont placées sur le bus de données DB. La seule difficulté consiste pour le fraudeur à savoir à quel moment précis ces données sont présentes sur le bus de données DB, afin de les identifier dans le flot de données qui transitent sur ce bus lors du fonctionnement du circuit électronique.

Or, on a remarqué que le courant électrique consommé par le circuit électronique en cours de fonctionnement n'est pas constant mais présente des variations en fonction, notamment, des opérations de lecture effectuées dans les différentes mémoires du circuit électronique. En effet, les cellules mémoires des différentes mémoires présentent une impédance qui, dans une certaines mesure, dépend de l'état programmé ou effacé de la cellule, mais qui, dans une plus large mesure, est différente d'un type de mémoire à l'autre.

A la figure 2, une courbe 21 représente ainsi les variations en fonction du temps du courant électrique I consommé par le microcontrôleur en fonctionnement. Ce courant peut prendre différentes valeurs croissantes  $I(Reg)$ ,  $I(ROM)$ ,  $I(RAM)$ ,  $I(EEPROM)$  pour des opérations de lecture, respectivement dans le registre Reg, la mémoire ROM, la mémoire RAM ou la mémoire EEPROM. Par conséquent il suffit au fraudeur d'observer la valeur instantanée du courant électrique consommé par le microcontrôleur (en disposant un moyen adapté, tel qu'un ampèremètre en série entre une borne

d'alimentation du lecteur prévue pour l'alimentation électrique de la carte à puce et la pastille de contact correspondante de celle-ci) et de relever les données présentes sur le bus de données DB au moment où ce courant présente la valeur  $I_{(EEPROM)}$ , pour connaître les données confidentielles lues dans la mémoire EEPROM.

Afin d'empêcher ce type de fraude, on a déjà proposé des moyens pour masquer les variations du courant consommé par le circuit électronique en cours de fonctionnement, qui agissent pour faire en sorte que le courant consommé par le circuit électronique en fonctionnement ait en permanence une même valeur  $I_{const}$ . Celle-ci est supérieure à la plus grande valeur du courant normalement consommé par le circuit électronique en fonctionnement. Un exemple de tels moyens est décrit dans la demande de brevet EP-A-0 500 461, où ils sont utilisés pour masquer les variations du courant consommé lors d'une opération de lecture dans une mémoire qui sont dues à l'état programmé ou effacé des cellules de la mémoire. Ils comprennent par exemple une source de courant constant (de valeur  $I_{const}$ ) connectée en série avec les cellules mémoires entre la borne d'alimentation positive  $V_{cc}$  et la masse, ainsi qu'une résistance connectée en parallèle avec les cellules mémoire.

A la figure 2, la courbe du courant (constant, de valeur  $I_{const}$ ) consommé par le circuit électronique selon cet art antérieur est représentée par une courbe 22, qui correspond sensiblement à une ligne horizontale. Les faibles ondulations des courbes 21 et 22 correspondent à des impédances parasites dans le circuit électronique.

Cette solution connue présente néanmoins l'inconvénient d'augmenter la consommation du circuit électronique de façon importante. En effet le courant consommé par le circuit électronique en fonctionnement est en permanence égal à la valeur  $I_{const}$  qui est supérieure à la valeur maximum du courant consommé en soi par le circuit électronique en fonctionnement. Cette consommation élevée engendre des problèmes liés notamment à l'élévation de la température par effet Joule dans le circuit électronique.

L'invention vise à pallier les inconvénients précités des circuits électroniques de l'état de la technique.

A cet effet, l'invention propose un procédé de gestion d'un circuit électronique, par exemple du type comprenant une mémoire pour le stockage d'informations confidentielles, caractérisé en ce qu'il comprend le masquage des variations du courant électrique consommé par le circuit électronique, pendant une fraction du temps seulement, et en tout état de cause pendant la ou les portions du temps pendant lesquelles est exécutée une instruction portant sur des données confidentielles.

Notamment, mais pas uniquement, le procédé comprend le masquage des variations du courant consommé par le circuit électronique pendant une portion du temps pendant laquelle est exécutée, entre autres, une instruction de lecture dans la mémoire.

L'invention propose également un circuit électronique, notamment un microcontrôleur, par exemple du type comprenant une mémoire pour le stockage d'informations confidentielles, qui comporte des moyens de masquage des variations du courant électrique consommé par le circuit électrique en fonctionnement ainsi que des moyens d'activation et de désactivation sélectives des moyens de masquage.

Par l'adjectif "sélectives", on entend une activation et une désactivation délibérées, c'est à dire provoquées délibérément lorsqu'elles sont nécessaires à l'obtention de l'effet technique recherché, à savoir masquer les variations du courant consommé par le circuit électronique lorsqu'une opération portant sur des données confidentielles est exécutée mais ne pas les masquer en permanence de manière à ne pas excessivement augmenter la consommation électrique moyenne du circuit électronique.

Grâce à l'invention, le courant consommé par le circuit électronique n'est égal à une valeur constante maximum que pendant une fraction du temps seulement, en sorte que la consommation globale du circuit électronique est réduite.

Cependant, le masquage des variations du courant consommé par le circuit électronique est effectif pendant les portions

du temps où, notamment, des instructions de lecture de données confidentielles sont effectuées, en sorte qu'il est très difficile voire impossible de détecter le moment exact où ces données sont présentes sur le bus de données DB.

5 D'autres caractéristiques et avantages de l'invention apparaîtront encore à la lecture de la description qui va suivre. Celle-ci est purement illustrative et doit être lue en regard des dessins annexés sur lesquels on a représenté :

- à la figure 1, déjà analysée, le schéma de l'architecture interne d'un circuit électronique selon l'art antérieur ;
- à la figure 2, également déjà analysée : des courbes du courant consommé par le circuit électronique en fonctionnement, respectivement sans masquage des variations et avec masquage des variations selon l'art antérieur ;
- 15 - à la figure 3, le schéma de l'architecture interne d'un circuit électronique selon l'invention ;
- à la figure 4 : le schéma de moyen de masquage selon l'invention ;
- à la figure 5 : l'organigramme d'une séquence 20 d'instructions d'un programme de gestion d'un circuit électronique selon l'invention ;
- à la figure 6 : des courbes du courant consommé par le circuit électronique en fonctionnement, respectivement sans masquage des variations et avec masquage des variations 25 selon l'invention.

A la figure 3, sur laquelle les mêmes éléments qu'à la figure 1 portent les mêmes références, on a représenté un circuit électronique selon l'invention. Il comporte une unité centrale de traitement CPU, une première mémoire non volatile 30 ROM (qui est une mémoire à lecture seule) pour le stockage permanent d'un programme de gestion exécutable par l'unité centrale de traitement CPU et une seconde mémoire non volatile EEPROM (qui est une mémoire électriquement programmable et effaçable à lecture seule) pour le stockage permanent 35 d'informations confidentielles. Il comporte en outre une mémoire volatile RAM (qui est une mémoire à accès aléatoire) pour le stockage temporaire d'informations liées au fonctionnement du circuit. En outre, ils comprennent encore au

moins un registre Reg pour le stockage d'une information binaire.

Selon l'invention, le circuit électronique comporte en outre un tel registre, portant la référence 10, qui a une fonction particulière selon l'invention. En fonction de l'état de ce registre, les moyens de masquage des variations du courant consommé par les mémoires ROM, RAM et/ou EEPROM sont activés ou désactivés. Dit autrement, il est stocké dans le registre 10 une valeur logique déterminée ou la valeur logique complémentaire, pour respectivement activer ou désactiver les moyens de masquage du courant consommé par le circuit électronique.

Des moyens de masquage sont représentés à la figure 4, en ce qui concerne la mémoire EEPROM. Ces moyens de masquage comprennent schématiquement une source de courant IC1 connectée en série avec la mémoire EEPROM par l'intermédiaire d'un interrupteur SW, entre un noeud d'alimentation positive recevant un potentiel d'alimentation positif Vcc d'une part et la masse d'autre part. On note A le noeud entre l'interrupteur SW et la mémoire EEPROM. Une résistance R1 est connectée en parallèle sur les bornes de la mémoire EEPROM (entre le noeud A et la masse).

Dans un premier état de l'interrupteur SW, correspondant à l'activation des moyens de masquage, le noeud A est relié à la borne négative de la source de courant IC1, en sorte que le courant J1 délivré par la source IC1 s'écoule à travers la mémoire EEPROM sous forme d'un courant I3 d'une part, et/ou à travers la résistance R1 sous forme d'un courant I1 d'autre part. En tout état de cause, la somme I1+I3 des courants I1 et I3 est constante et est égale au courant J1, même lorsqu'une opération de lecture dans la mémoire EEPROM est effectuée.

Comme on l'aura compris, la valeur de R1 doit être comprise entre la valeur minimum et la valeur maximum de l'impédance de la mémoire EEPROM, afin de jouer un rôle de compensation des variations du courant I3 au cours du fonctionnement du microcontrôleur. Bien entendu, la valeur de J1 doit être supérieure à la valeur maximum du courant I3 au cours du fonctionnement du microcontrôleur (cette valeur maximum est

atteinte lors d'une opération effectuée dans la mémoire EEPROM). Dans un cas limite, le courant I1 peut éventuellement être nul.

Dans un second état de l'interrupteur SW, correspondant à 5 la désactivation des moyens de masquage, le noeud A est connecté directement à la broche recevant le potentiel d'alimentation Vcc, en sorte que la source IC1 ne débite aucun courant dans la mémoire EEPROM ni dans la résistance R1 (cette source est éteinte). Un courant I3 et/ou un courant I1 10 s'écoulent respectivement à travers la mémoire EEPROM et/ou la résistance R1 directement depuis la borne d'alimentation délivrant le potentiel Vcc. Leurs valeurs, éventuellement très faibles, sont fonction de l'impédance de la mémoire EEPROM par rapport à R1. La somme I1+I3 des courants I1 et I3 n'est pas 15 constante. Notamment, elle varie lorsqu'une opération de lecture dans la mémoire EEPROM est effectuée. Elle peut être très faible, notamment lorsque aucune opération n'est effectuée dans la mémoire EEPROM. En tout état de cause, elle est inférieure à la valeur du courant J1 du premier cas ci-dessus, 20 en sorte qu'il est obtenu une économie du courant consommé par la microcontrôleur.

La structure des moyens de masquage représentés à la figure 3 est purement schématique. De tels moyens peuvent être réalisés concrètement de toute manière appropriée, notamment à 25 l'aide d'une circuiterie à base de transistors, par exemple des transistors MOS.

De retour à la figure 3, on comprend que chaque mémoire du microcontrôleur, en l'occurrence les mémoires RAM, ROM et EEPROM, sont dotées de moyens de masquage tels que présentés à 30 la figure 4. L'état de l'interrupteur SW de ces moyens de marquage est commandé par la valeur logique mémorisée par le registre 10. Dit autrement, l'activation ou la désactivation des moyens de masquage des mémoires du microcontrôleur est fonction de l'état du registre 10. On va maintenant décrire la 35 façon dont cet état est modifié afin d'activer ou de désactiver les moyens de masquage.

A la figure 5 on a représenté une séquence d'instructions d'un programme de gestion du microcontrôleur, qui est stocké

dans la mémoire ROM. Ce programme est écrit en fonction de l'application du microcontrôleur et est stocké dans la mémoire ROM. De manière connue en soi, les instructions contenues dans ce programme sont exécutées séquentiellement lors du 5 fonctionnement du microcontrôleur.

Entre une instruction de début de programme START et une instruction de fin de programme END, le programme comprend une séquence d'instructions  $Inst_1, \dots, Inst_n$ . Parmi ces instructions une instruction particulière,  $Inst_i$ , a pour effet 10 d'inscrire une valeur logique particulière dans le registre 10, par exemple la valeur logique 1, en sorte que l'interrupteur SW est mis dans le premier état précité. Une autre instruction  $Inst_j$  subséquente à l'instruction  $Inst_i$  dans la séquence, a pour fonction d'inscrire la valeur logique 15 complémentaire dans le registre 10, à savoir par exemple la valeur logique 0, en sorte que l'interrupteur SW est mis dans le second état précité.

Comme on l'aura compris, ces deux instructions  $Inst_i$  et  $Inst_j$  sont insérées dans la séquence d'instructions du 20 programme de gestion de manière à encadrer, entre autres, une instruction de lecture dans la mémoire EEPROM. De cette façon les données confidentielles lues dans la mémoire EEPROM transitent sur le bus de données DB alors que les moyens de masquage J1,SW,R1 des mémoires sont activés.

Il va sans dire que les moyens de masquage sont activés par 25 l'instruction  $Inst_i$  suffisamment tôt avant l'instruction de lecture, et sont désactivés par l'instruction  $Inst_j$  suffisamment longtemps après ladite instruction de lecture, pour que le masquage des variations du courant consommé par le 30 circuit électronique soit efficace. Dit autrement, le procédé selon l'invention comprend le masquage des variations du courant consommé par le circuit électronique pendant une portion du temps pendant laquelle, entre autres, une instruction de lecture dans la mémoire EEPROM est exécutée. 35 Mais le masquage doit être suffisamment long pour que l'opération de lecture dans la mémoire EEPROM ne soit pas facilement décelable. Il est évident que si les moyens de

masquage n'étaient activés que pendant l'opération de lecture, l'effet de masquage recherché ne serait pas obtenu.

A l'inverse, la portion du temps pendant laquelle les moyens de masquage sont activés, i.e., la portion du temps entre les instructions Inst<sub>i</sub> et Inst<sub>j</sub>, est suffisamment courte pour que soit substantielle l'économie de courant consommé par le circuit électronique par rapport à l'utilisation de moyens de masquage permanents conformément à l'art antérieur.

C'est pourquoi, on dit que l'activation et la désactivation des moyens de masquage des variations du courant consommé par le circuit électronique sont sélectives.

A la figure 6, qui est à comparer à la figure 2, une courbe 61 représente, en fonction du temps, le courant électrique I consommé par le circuit électronique en fonctionnement selon le principe de l'invention. Les moyens de masquage des mémoires du microcontrôleur sont activés à un instant  $t_i$  et sont désactivés à un instant ultérieur  $t_j$  respectivement par l'exécution de l'instruction Inst<sub>i</sub> et par l'exécution de l'instruction Inst<sub>j</sub>.

Dans la portion du temps comprise entre ces deux instants  $t_i$  et  $t_j$ , le courant consommé par le circuit électronique est constant et vaut Iconst. Notamment, il ne varie pas en fonction des opérations de lecture effectuées dans les mémoires ROM, RAM et/ou EEPROM. De cette manière un fraudeur ne parvient pas à savoir à quel moment précis les données présentes sur le bus de données du microcontrôleur correspondent au code personnel de la carte à puce. Une courbe 62, en traits discontinus, montre ce que serait l'allure du courant consommé par le microcontrôleur entre les instants  $t_i$  et  $t_j$  sans l'activation des moyens de masquage selon l'invention.

Dans l'exemple, la valeur Iconst correspond sensiblement à la somme des courants J<sub>1</sub> des moyens de masquage des mémoires ROM, RAM et EEPROM activés simultanément entre les instants  $t_i$  et  $t_j$ . On notera que les courants J<sub>1</sub> n'ont pas forcément la même valeur pour chacune des mémoires ROM, RAM et EEPROM. En

outre, il n'est pas indispensable que des moyens de masquage soient prévus pour chacune des mémoires du microcontrôleur.

Dans un autre mode de réalisation, des moyens de masquage peuvent être disposé ailleurs que dans les mémoires. Par 5 exemple, on peut prévoir des moyens de masquage uniques, disposés directement à proximité de la pastille de contact prévue pour l'alimentation électrique de la carte à puce. Néanmoins, des moyens de masquage uniques disposés de cette manière sont plus faciles à déjouer par un fraudeur.

10 L'invention a été décrite ci-dessus en ce qui concerne le masquage des variations du courant consommé par le circuit électronique lors de l'exécution, entre autres, d'une instruction de lecture dans une mémoire de stockage d'informations confidentielles. Mais, bien entendu, elle ne se 15 limite pas à ce cas. Au contraire, elle s'applique au masquage de des variations du courant consommé par le circuit électronique lors de l'exécution, entre autres, de toute instruction portant sur des données confidentielles.

**REVENDICATIONS**

1. Procédé de gestion d'un circuit électronique, caractérisé en ce qu'il comprend la mise en oeuvre de moyens de masquage des variations du courant électrique (I) consommé par le circuit électronique en fonctionnement, le procédé comprenant les étapes : a) d'activation sélective des moyens de masquage et b) de désactivation sélective des moyens de masquage, l'intervalle entre l'activation et la désactivation des moyens de masquage occupant une fraction ( $t_i-t_j$ ) seulement du temps de gestion, cette fraction couvrant en tout état de cause la ou les portions du temps pendant lesquelles est exécutée une instruction portant sur des données confidentielles.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend le masquage des variations du courant consommé par le circuit électronique pendant une portion du temps pendant laquelle est exécutée, entre autres, une instruction de lecture dans une mémoire (EEPROM) pour le stockage de données confidentielles.

3. Procédé selon la revendication 1 ou selon la revendication 2, caractérisé en ce que les moyens de masquage des variations du courant (I) consommé par le circuit électrique en fonctionnement sont activés par une première instruction ( $Inst_i$ ) et sont désactivés par une seconde instruction ( $Inst_j$ ) subséquente d'un programme de gestion du circuit électronique, ces instructions encadrant une instruction portant sur des données confidentielles.

4. Procédé selon la revendication 3, caractérisé en ce que la première instruction ( $Inst_i$ ) et la seconde instruction ( $Inst_j$ ) provoquent respectivement l'écriture d'une valeur logique déterminée et l'écriture de la valeur logique complémentaire dans un registre (10) du circuit électronique.

5. Circuit électronique, notamment un microcontrôleur, du type comprenant une mémoire pour le stockage d'informations confidentielles, caractérisé en ce qu'il comporte des moyens de masquage des variations du courant électrique consommé par le circuit électrique en fonctionnement ainsi que des moyens

d'activation et de désactivation sélectives des moyens de masquage.

6. Circuit électronique selon la revendication 5,  
5 caractérisé en ce qu'il comprend un registre (10) dans lequel  
est inscrite une valeur logique déterminée ou la valeur  
logique complémentaire, pour respectivement activer ou  
désactiver les moyens de masquage du courant consommé par le  
circuit électronique.

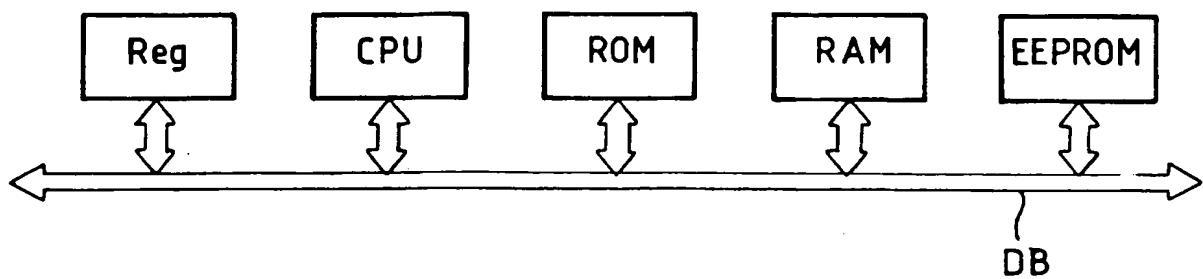
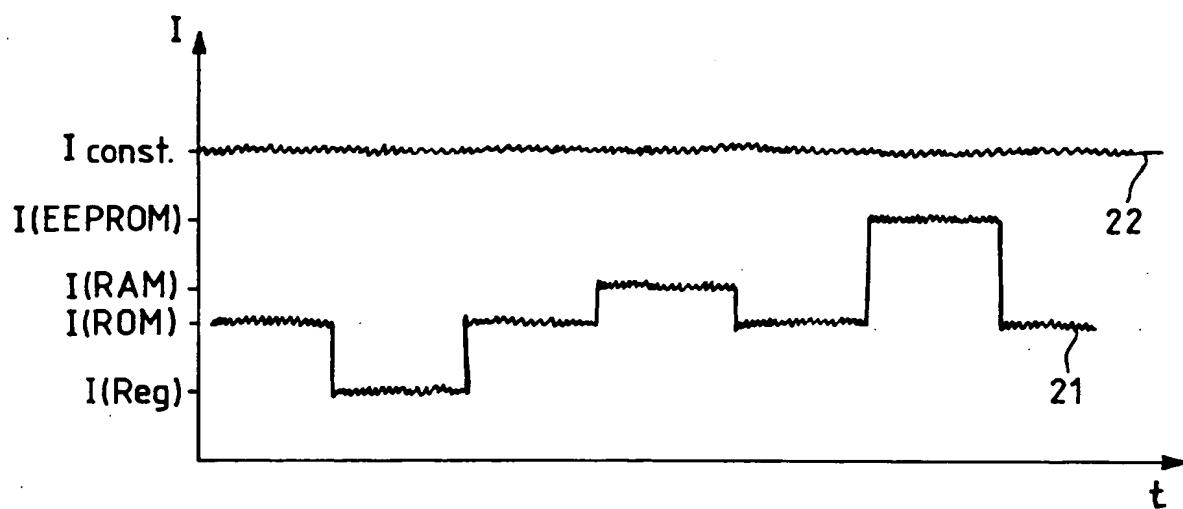
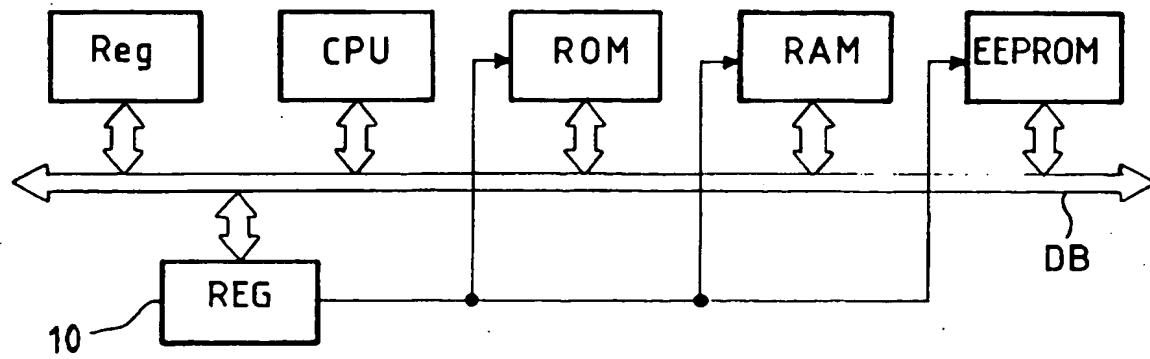
10

7. Circuit électronique selon la revendication 6,  
caractérisé en ce qu'il comporte une unité centrale de  
traitement (CPU), une première mémoire non volatile (ROM) pour  
le stockage permanent d'un programme de gestion exécutable par  
15 l'unité centrale de traitement (CPU) et une seconde mémoire  
non volatile (EEPROM) pour le stockage permanent  
d'informations confidentielles.

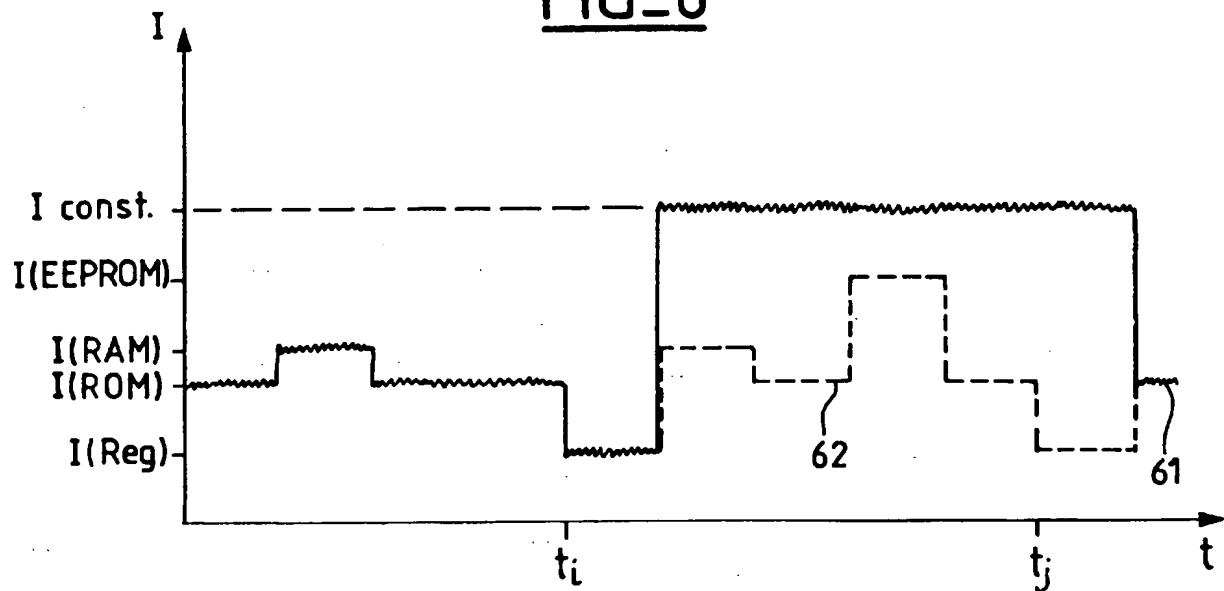
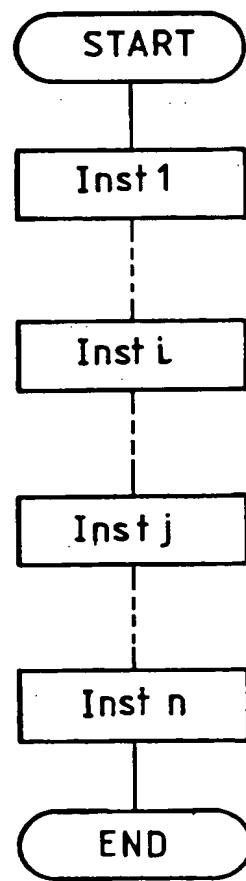
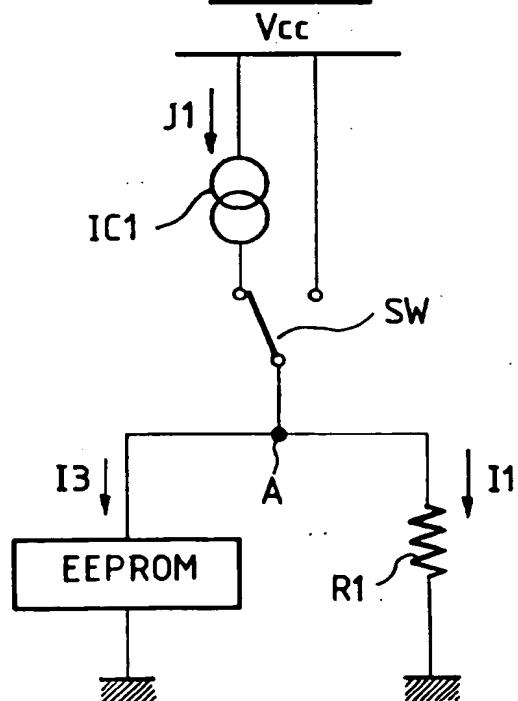
8. Circuit électronique selon la revendication 7,  
20 caractérisé en ce que le programme de gestion comporte une  
première instruction ( $Inst_i$ ) et une seconde instruction  
( $Inst_j$ ) pour provoquer respectivement l'écriture d'une valeur  
logique déterminée et l'écriture de la valeur logique  
complémentaire dans le registre (10), cette première et cette  
25 seconde instructions encadrant dans la séquence d'instructions  
du programme de gestion une instruction portant sur des  
données confidentielles, notamment une instruction de lecture  
dans la seconde mémoire non volatile (EEPROM).

30

1/2

FIG\_1FIG\_2FIG\_3

2 / 2

FIG\_6FIG\_5FIG\_4

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL  
de la  
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE  
PRELIMINAIRE

établi sur la base des dernières revendications  
déposées avant le commencement de la recherche

2793904

N° d'enregistrement  
national

FA 580068  
FR 9906499

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	EP 0 368 727 A (SGS THOMSON MICROELECTRONICS) 16 mai 1990 (1990-05-16) * abrégé * * colonne 1, ligne 1 - colonne 3, ligne 11 * ---	1-8
A	WO 97 33217 A (UGON MICHEL ; BULL CP8 (FR)) 12 septembre 1997 (1997-09-12) * le document en entier * ---	1-8
A	FR 2 757 972 A (BULL CP8) 3 juillet 1998 (1998-07-03) * abrégé * * page 4, alinéa 1 * -----	1-8
DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)		
G06F G11C		
1	Date d'achèvement de la recherche	Examinateur
	10 avril 2000	Powell, D
CATEGORIE DES DOCUMENTS CITES		
X : particulièrement pertinent à lui seul		T : théorie ou principe à la base de l'invention
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie		E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général		D : cité dans la demande
O : divulgarion non-écrite		L : cité pour d'autres raisons
P : document intercalaire		& : membre de la même famille, document correspondant